NASA Procedural Requirements

COMPLIANCE IS MANDATORY

NPR 8705.5A
Effective Date: June 07, 2010
Expiration Date: June 07, 2015

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: Technical Probabilistic Risk Assessment (PRA) Procedures for Safety and Mission Success for NASA Programs and Projects

Responsible Office: Office of Safety and Mission Assurance

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | AppendixA | AppendixB | AppendixC | ALL |

Chapter 1. Introduction

1.1 Background

1.1.1 A PRA is a structured, logical analysis methodology that is used for identifying and assessing risks in a variety of applications including complex technological systems. In general, a PRA provides a modeling framework that interfaces with or includes the various disciplines used to conduct health, safety, and mission assurance analyses including hazard analysis, failure mode and effects analysis, and reliability analysis. A PRA draws upon the relevant collection of qualitative and quantitative information and models that are developed as part of design and assurance activities.

1.1.2 A PRA is applicable to all program/project life-cycle phases: formulation (Pre-Phase A - Phase B), implementation (Phase C - Phase E), and closeout (Phase F). The scope, level of detail and type of information that are necessary, and the types of scenarios modeled may vary during the assessment of each life-cycle phase and its intended application. A PRA will have varying degrees of complexity and fidelity depending on the program/project life-cycle phase and the decisions being supported. High-level PRAs performed during formulation and early design may be used to compare and establish meaningful safety, health, and performance requirements for mission and architectural concepts. Later in the design, more focused PRAs may be performed to compare risks associated with proposed design solutions. As the program/project nears implementation, the PRA grows in complexity and fidelity to provide an integrated model of an entire mission or facility, including its architectural, mechanical, human, and software components.

1.1.3 NPD 1000.5, Policy for NASA Acquisition, requires the incorporation of a risk-informed acquisition process that includes the assessment of technical, safety, and health risks among others. In addition, for each life-cycle phase and application, PRA facilitates Agency risk management activities required by NPD 7120.4, Program/Project Management, and NPR 8000.4, Agency Risk Management Procedural Requirements. Risk analyses of decision alternatives that include the quantification and comparison of safety, health, and technical performance measures are used in the risk-informed decision making (RIDM) process. When decision alternatives are selected to define a program or project, a PRA is conducted to characterize weaknesses and vulnerabilities in design and implementation that can adversely impact safety and health, performance, and mission success. Those events that contribute most to risk and uncertainty can be identified by the PRA and provide the focus for further assessment and risk management strategies. These risk management activities can reveal where alternatives, changes in design and operation, and/or cost-effective expenditure of resources can be made to improve design and operation and inform the decision-makers of uncertainties that may need to be addressed.

1.1.4 The Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners is a companion document to this NPR and provides further details on PRA methodology for aerospace applications. Many references are made to this companion document for practical advice on performing PRAs.

1.2 PRA Characteristics

1.2.1 PRA is applied to identify and evaluate risks affecting safety and health; i.e., having a potential for injury or illness, loss of life, damage, or unexpected loss of equipment, as well as those affecting the ability to reliably meet mission objectives (e.g., due to equipment failure).

1.2.2 A PRA characterizes risk in terms of three basic questions: (1) What can go wrong? (2) How likely is it? and (3) What are the consequences? The PRA process answers these questions by systematically identifying, modeling, and quantifying scenarios that can lead to undesired consequences, considering uncertainties in the progression of such scenarios due to both variations of, and limited knowledge about, the system and its environment. The PRA integrates models based on systems engineering, probability and statistical theory, reliability and maintainability engineering, physical and biological sciences, decision theory, and expert elicitation. The collection of risk scenarios allows the dominant contributors to risk and areas of uncertainty about risk to be identified.

1.2.3 PRA generally consist of complex chains of events (or scenarios), each of which can lead to an undesired consequence or end state. Examples of such events include failures of hardware and software system elements, human actions or lack thereof, and phenomenological events such as degradation or debris impacts. Complex scenarios may include events whose implications separately appear to be slight or insignificant but collectively can combine and interact to cause high severity consequences. The total probability from the set of scenarios modeled may also be non-negligible even though the probability of each scenario is small.

1.2.4 The assessment normally takes place in the context of safety, health, and mission success criteria that specify a minimum required level of confidence that loss of life and equipment will be avoided, and mission objectives will be achieved. While elements of

such requirements may be allocated to other disciplines; e.g., hardware reliability, the PRA provides an integral modeling framework in which various elements can be represented.

1.2.5 A PRA is conducted using a systematic process to assess operational objectives, application(s), and scope; model scenarios that can lead to undesired consequences or end states; quantify scenario probabilities and consequences, as applicable, including the characterization of uncertainty; and provide and interpret results for the decision(s) being supported. Documentation and communication are also important parts of the PRA process.

1.2.6 Two examples of PRAs are provided in the Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners.

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | AppendixA | AppendixB | AppendixC | ALL |

| NODIS Library | Program Management(8000s) | Search |

DISTRIBUTION:
NODIS